THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, November 16, 2020

The China Initiative: Year-in-Review (2019-20)

On the two-year anniversary of the Attorney General's China Initiative, the Department continues its significant focus on the Initiative's goals and announced substantial progress during the past year in disrupting and deterring the wide range of national security threats posed by the policies and practices of the People's Republic of China (PRC) government.

"In the last year, the Department has made incredible strides in countering the systemic efforts by the PRC to enhance its economic and military strength at America's expense," said Attorney General William P. Barr. "While much work remains to be done, the Department is committed to holding to account those who would steal, or otherwise illicitly obtain, the U.S. intellectual capital that will propel the future."

"The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt," said FBI Director Christopher Wray. "The FBI opens a new China-related counterintelligence case nearly every 10 hours and we'll continue our aggressive efforts to counter China's criminal activity."

Established in November 2018, the Initiative identified a number of goals for the Department, ranging from increased focus on the investigation and prosecution of trade secret theft and economic espionage, to better countering threats posed by Chinese foreign investment and supply chain vulnerabilities.

Prioritize investigations of economic espionage and trade secret theft

The Initiative prioritizes use of the Department's core tool, criminal investigation and prosecution, to counter economic espionage and other forms of trade secret theft. In the past year, the Department charged three economic espionage cases (in which the trade secret theft was intended to benefit the Chinese government), bringing the total to five since the China Initiative was first announced. Overall, since the Initiative was announced, we have charged more than 10 cases in which the trade secret theft had some alleged nexus to China, and we obtained guilty pleas of three defendants in those cases over the past year.

To take one example, the Department announced the China Initiative on the same day that it unsealed criminal charges against United Microelectronics (UMC), the Chinese state-owned enterprise Fujian Jinhua, and several individual defendants, for economic espionage that victimized Micron Technology, Inc., a leading U.S. semiconductor company.

"The United Microelectronics case is a glaring example of the PRC's 'rob, replicate, and replace' strategy, in which it robs a U.S. institution of its intellectual capital, replicates the stolen technology, and then endeavors to replace the U.S. institution on the Chinese and then the global market," said John Demers, Assistant Attorney General for National Security. "Thanks to the dedication and diligence of prosecutors and FBI agents, UMC pleaded guilty to criminal trade secret theft and agreed to pay a fine of $60 million, the second largest fine in a trade secret case, and to cooperate in the pending prosecution of its co-defendants."

The National Counterintelligence Task Force, co-led by the FBI, launched its first major campaign in 2020, devoted to protecting U.S. technology and research from the Chinese government and its proxies. This is a further step in the

FBI's and Department's efforts to enlist all appropriate partners in ensuring integrity in government-funded programs and defeating economic espionage and theft of trade secrets.

Develop an enforcement strategy for non-traditional collectors

At the outset, the Department identified academia as one of our most vulnerable sectors, because its traditions of openness, and the importance of international exchanges to the free flow of ideas, leave it vulnerable to PRC exploitation. The Department has pursued a two-pronged strategy of raising awareness on campuses of the threats posed by China (and the importance of implementing a security program to detect them) and prosecuting researchers who have deliberately deceived authorities about their ties to China, which deprives institutions of the ability to screen for conflicts of interest and commitment, or otherwise exploited their access.

For example, the PRC has used talent programs to encourage the transfer of technical expertise from the United States, and elsewhere in the world, to benefit the PRC's economic and military development. Talent recruits generally sign contracts with the PRC sponsor-entity that obligate them to produce scientific outputs; to publish the results of their work in the name of the PRC beneficiary; to allow the PRC beneficiary to assert intellectual property rights over their outputs; and to recruit other researchers into the programs, among other obligations.

In exchange, the talent recruits may receive lucrative compensation packages, prestigious titles, and custom-built laboratories.

"While membership in these talent programs is not *per se* illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to work in the interest of the Chinese Communist Party," said Adam S. Hickey, Deputy Assistant Attorney General, National Security Division.

The Initiative brings together resources from across the Department, including the National Security, Criminal, Tax, and the Civil Divisions to address this unique challenge fairly and effectively. In the past year, Department prosecutors have brought fraud, false statements, tax, smuggling and other charges against ten academics affiliated with research institutions across the country. To date, prosecutors have obtained convictions in three of those cases.

This year, the FBI and Department prosecutors also exposed six individuals, studying in the United States, found to be connected to People's Liberation Army military institutes, who concealed their affiliations from the State Department when applying for research visas to study at U.S. universities. In one of those cases, the Department alleged that a PLA officer was being tasked by superiors in the PRC to obtain information that would benefit PLA operations. In another case, a PLA medical researcher stands accused of following orders to observe lab operations at a U.S. university, which received funding from the U.S. government, in order to replicate those operations in the PRC.

In each of the cases, the defendants are accused of concealing their PLA affiliations in order to obtain visas that allowed them to travel to the United States. After the FBI conducted interviews this summer that led to charges in those cases and the State Department closed the PRC's Houston Consulate, a large number of undeclared, PLA-affiliated Chinese researchers fled the United States.

Those six examples are just part of the interagency effort to protect academia and taxpayer-funded research. The FBI and Department have been collaborating with federal grant-making agencies, the Joint Committee on the Research Environment, the major academic associations, the Academic Security and Counter Exploitation working group, and other appropriate entities, as well as hundreds of individual universities nationwide.

Counter malicious cyber activity

The Department continues to expose and disrupt efforts by the PRC government to steal our intellectual property and our personally identifiable information (PII) through computer intrusions. During the past year, we charged hackers working for the People's Liberation Army with the 2017 Equifax intrusion and others associated with the Ministry of State Security (MSS) in relation to global computer intrusion campaigns targeting biomedical companies conducting COVID-19-related research, engineering firms, and software makers. One such MSS case resulted in the arrest of two conspirators in Malaysia. Two of these cases highlighted China's development into a safe harbor for criminal hackers who also work for the PRC. The Department disrupted these cyber threats in coordination with the private sector, using

legal process to seize control of hacking infrastructure while the private sector removed other infrastructure from their platforms.

In May, the FBI, in conjunction with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, also issued a public announcement to raise awareness of the threat to COVID-19 research by PRC-affiliated cyber actors and offer advice on better protecting that research from thefts.

Counter malign foreign influence

The Department has used the Foreign Agents Registration Act ("FARA"), which requires those acting to influence public policy and opinion on behalf of a foreign individual or entity, to improve transparency and expose China's foreign influence efforts. Over the past year, the Department opened a record number of FARA investigations overall and doubled the number of new registrants and new foreign principals registering annually as of 2016. That includes obtaining a record number of registrations from Chinese media companies. The Department also notified a registered Chinese media company that its filings were deficient because they failed to fully disclose its activity in the United States and failed to properly label its informational materials. The media entity remedied those deficiencies shortly thereafter.

Through its outreach efforts to universities, the Department has highlighted the need to protect foreign students studying in the United States from coercive efforts by the Communist Party to censor the freedom of thought and expression that all students here should enjoy.

In late 2019, the FBI's Foreign Influence Task Force formally established a new unit devoted specifically to understanding and defeating the malign foreign influence threat from the Chinese government and its proxies.

Counter foreign intelligence activities

The Department has achieved a number of successes in the last year in countering China's foreign intelligence activities. China has been targeting former members of the U.S. intelligence community for recruitment, and the Department has been holding accountable individuals who succumb to their efforts. In November 2019, a former CIA case officer was sentenced to 19 years in prison for conspiring to deliver national defense information to the PRC. In August 2020, another former CIA officer who had been tasked by the PRC was arrested on the same charge — the fourth former intelligence officer charged in the last three years for similar conduct.

The Department is particularly focused on disrupting the PRC government from using career networking and social media sites to target Americans, as well as holding those accountable who hide behind fake profiles to co-opt individuals on behalf of the PRC. As one part of this effort, the FBI, in partnership with the National Counterintelligence and Security Center, created an educational film, "The Nevernight Connection," which was released online in September 2020 to educate the public about the Chinese intelligence services' use of social media to spot and recruit persons of interest, especially current or former security clearance holders.

In March 2020, Xuehua (Edward) Peng was sentenced to 48 months in prison, and ordered to pay a $30,000 fine, for acting as an agent of the PRC's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital cards containing classified information from a source in the United States to the MSS operatives in China.

In October 2020, Jun Wei Yeo was sentenced to 14 months in prison for acting within the United States as an agent of the MSS recruiting Americans, including U.S. military and government employees with high-level clearances. Yeo concealed his MSS affiliation from his American targets and used career networking sites and a false consulting firm to lure them to write papers which he ultimately passed to his MSS handlers.

In October 2020, eight defendants were charged with conspiring to act in the United States as illegal agents of the PRC, six of whom also face related charges of conspiring to commit interstate and international stalking. According to the complaint, the defendants participated in an international campaign to threaten, harass, surveil and intimidate a resident of New Jersey and his family in order to force them to return to the PRC as part of an international effort by the PRC government known as "Operation Fox Hunt" and "Operation Skynet."

In furtherance of the operation, the PRC government targets Chinese individuals living in foreign countries that the PRC government alleges have committed crimes under PRC law and seeks to repatriate them to the PRC to face charges, rather than rely upon proper forms of international law enforcement cooperation.

Foreign investment reviews and telecommunications security

Beyond criminal enforcement, the Department worked to protect our national assets from national security risks posed by entities, subject to PRC influence, that seek to invest in U.S. companies or integrate into our supply chains.

In April, the Department assumed the permanent chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, established by the President through Executive Order (EO), in 2020. This organization, also known as "Team Telecom," is an interagency group that reviews telecommunications, submarine cable landing, wireless, broadcast license, and other applications referred by the Federal Communications Commission (FCC), to identify and address risks to national security and law enforcement. In the first 90 days after the Executive Order, the Department led Team Telecom to resolve more than half of the cases then pending review.

Team Telecom recommended that the FCC revoke and terminate the international telecommunications licenses held by the U.S. subsidiary of a PRC state-owned telecommunications company, China Telecom, the first revocation ever recommended by Team Telecom on national security grounds. Team Telecom also recommended that the FCC partially deny a submarine cable application, to the extent it sought a direct connection between the United States and Hong Kong.

Following the President's 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, the Department has worked with the Commerce Department to develop regulations implementing the EO and has identified vulnerable areas of critical infrastructure that are ripe for investigation under the EO.

The Department also worked to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), which improved the authorities of the Committee on Foreign Investment in the United States (CFIUS). During the previous year, the Department co-led a record number of significant CFIUS matters, on an annualized basis, including the investigation of the acquisition of a U.S. hotel management software company by a Chinese company, which the President prohibited, for just the sixth time in CFIUS history. Under FIRRMA, the FBI continued to provide analytical assistance to support CFIUS's decision-making and identify high-risk non-notified transactions.

With its increased resources, NSD has played a significant role in CFIUS enforcement, leading the Committee to assess just the second penalty in its history, for failing to secure sensitive personal data in violation of a 2018 interim CFIUS order. NSD also dedicated personnel to identify transactions of concern that were not voluntarily filed with CFIUS and developed a program to identify bankruptcy cases that could implicate national security concerns. The bankruptcy program helps to protect U.S. assets from predatory acquisitions, including PRC acquisitions that could impact our national security, which is particularly important in light of the economic impact of COVID-19.

Education and outreach

The success of the China Initiative is not measured by criminal cases and administrative actions alone, however. Outreach to businesses and academia is critical to helping America's national assets better protect themselves. For that reason, the Department disseminated outreach presentations for use by U.S. Attorneys in their Districts, which have been deployed at various events. The FBI sustained its engagement with the private sector through various programs, and it developed and disseminated an innovative Academia Field Guide to support focused outreach by its academic outreach coordinators in all 56 field offices. In the coming year, the Department, through the FBI and U.S. Attorneys' Offices, will continue to expand our partnerships outside the federal government, because the support of the American people is critical to our success. All of our efforts are on their behalf.

The Attorney General commends the professionals throughout the Department, including those who work at Main Justice, the FBI, and U.S. Attorney's Offices around the country, who are committed to meeting the goals of the China Initiative and encourage them to redouble their efforts in the upcoming year.

All defendants, in the cases mentioned herein, are presumed innocent until proven guilty beyond a reasonable doubt.

Topic(s):
National Security

Component(s):
Federal Bureau of Investigation (FBI)
National Security Division (NSD)
Office of the Attorney General

Press Release Number:
20-1238

Updated November 16, 2020